그리드 컴퓨팅 시스템에서의 양자내성암호 기반 사용자 인증 및 키 교환 프로토콜 구현 및 성능 측정

한재영[O], 황제현[*], 이재석[**], 이인희[***], 이영준[****], 이제원[*****], 김성욱[******]
[O]서울여자대학교 정보보호학과,
[*]수원대학교 컴퓨터학부,
[**]전남대학교 컴퓨터정보통신공학과,
[***]경북대학교 컴퓨터학부,
[****]세종대학교 정보보호학과,
[*****]NSHC 연구원,
[******]서울여자대학교 정보보호학과
e-mail: byobin26@gmail.com[O], jwlee@nshc.net[*****], kim.sungwook@swu.ac.kr[******]

Implementation and performance analysis of authentication and key exchange protocol with post-quantum cryptography in grid computing system

Jae-Yeong Han[O], Je-Hyun Hwang[*], Jae-Seok Lee[**], Young-Jun Lee[***],
In-Hee Lee[****], Je-Won Lee[*****], Sung-Wook Kim[******]
[O]Dept. of Information Security, Seoul Women's University,
[*]Division of Computer Science, The University of Suwon,
[**]Department of Computer Engineering, Chonnam National University,
[***]Dept. of Information Security, Sejong University,
[****]Department of Computer Science Kyungpook National University,
[*****]Researcher, NSHC,
[******]Dept. of Information Security, Seoul Women's University

● 요 약 ●

본 논문에서는 그리드 컴퓨팅에서의 안전한 통신을 위한 양자내성암호 기반 사용자 인증 및 키 교환 프로토콜을 구현하고 성능을 측정한다. 디지털 서명을 통해 사용자를 검증하고 암호키를 교환하여 신뢰할 수 있는 사용자들만이 그리드 컴퓨팅에 참여할 수 있도록 한다. 사용자 인증과 키 교환 과정에 NIST 선정 표준 양자내성암호인 ML-DSA와 ML-KEM을 적용하여 양자컴퓨터를 이용한 공격에도 안전할 것으로 기대된다. 본 논문에서는 양자내성암호를 적용한 프로토콜이 기존의 현대암호 기반 전자서명이나 키 교환 과정에 비해 양자내성과 동시에 준수한 사용성을 지녔음을 보인다. 이를 통해 그리드 컴퓨팅의 시스템의 P2P 특성에서 기인하는 보안 문제를 해결하고, 기존에 주로 내부망이나 실시간 스트리밍 서비스에서 활용되던 그리드 컴퓨팅의 인터넷 환경으로의 확장 가능성을 제시한다.

키워드: 양자내성암호(post-quantum cryptography), 그리드 컴퓨팅(grid computing), 디지털 서명(digital signature)

I. Introduction

양자컴퓨터의 발전으로 현대 컴퓨터로는 해결 불가능했던 난제들을 기반으로 하는 현대암호체계가 무력화될 수 있다. 양자컴퓨터의 위협에 대비하기 위해 미국 국립표준기술연구소(National Institute of Standards and Technology, NIST)는 2016년부터 키 캡슐화 메커니즘(Key Encapsulation Mechanism, KEM) 및 전자서명(Digital-Signature) 기능을 보유한 새로운 암호화 알고리즘의 표준화

를 위한 공모를 진행했다. 2023년 8월, NIST는 양자내성암호(Post-Quantum Cryptography, PQC) 알고리즘 표준 초안을 발표했다. 선정된 PQC 표준 초안은 키 캡슐화 메커니즘인 ML-KEM(CRYSTALS-Kyber)과 전자 서명인 ML-DSA (CRYSTALS-Dilithium), FN-DSA(FALCON), SLH-DSA (SPHINCS+)이다. 지속적인 양자컴퓨팅 기술의 발전에 따라 차세대 네트워크 통신에 대해 양자내성암호 적용을 고려해야 한다.

또한, AI 분야의 부상으로 인공지능 연산을 위한 고성능 컴퓨팅 수요가 증가하고 있으나 하드웨어 자원의 생산이 수요를 맞추지 못하고 있다. 이에 대한 방안으로 기존의 유휴 컴퓨팅 자원을 활용할 수 있는 그리드 컴퓨팅이 있다. 인터넷을 통해 시공간의 제약 없이 그리드 컴퓨팅이 가능하도록 하려면 통신 과정에서 데이터 도청, 탈취, 악성 사용자의 참여와 같은 사이버 공격을 방어해야 한다.

따라서 본 논문에서는 그리드 컴퓨팅 환경에서 양자내성암호를 적용한 인증 및 키 교환 프로토콜을 구현하고 성능을 분석한다. 이를 통해 사용자 인증 및 키 교환 과정에 기존 현대암호를 대체하는 양자내성암호의 적용 가능성을 제시한다.

II. Preliminaries

1. Related works

TLS 1.3 프로토콜에서 양자내성암호 적용 가능성에 관한 연구가 진행되었다. NIST에서 선정한 다양한 PQC 알고리즘들을 대상으로 TLS 1.3에 통합하기 위한 성능과 적합성을 평가한 결과, CRYSTALS-Kyber와 CRYSTALS-Dilithium을 TLS Handshake 단계에서 가장 좋은 성능을 가진 알고리즘으로 선정하였다[1].

그리드 컴퓨팅 기반 실시간 스트리밍 서비스의 취약점 및 대응 방안 연구에서는 그리드 컴퓨팅 시스템의 P2P 특성으로 인해 발생할 수 있는 보안 문제를 다루었다. 5가지의 공격 시나리오를 바탕으로 취약점을 도출하고, 공격 수행 시 하나의 전체 노드에 영향을 줄 수 있는 네트워크 웜처럼 동작할 수 있음을 증명하였다. 따라서 그리드 컴퓨팅 시스템을 활용할 경우 사용자 간의 인증과 데이터에 대한 무결성 검증의 필요성을 제기하였다[2].

2. Background

2.1 양자내성암호

양자내성암호는 양자컴퓨터를 이용한 공격으로부터 안전하다고 기대되는 암호 시스템이다. 주요한 양자내성암호는 그 바탕이 되는 수학적 난제 혹은 이론에 따라 Lattice-based(격자 기반), Multivariate-based(다변수 다항식 기반), Code-based(코드 기반), Isogeny-based(아이소제니 기반), Hash-based(해시 기반)의 5가지 종류로 나뉜다.

본 논문에서 다루는 ML-KEM과 ML-DSA 알고리즘은 모두 Lattice-based 양자내성암호이다.

2.1.1 ML-KEM

ML-KEM(Module Lattice-based Key-Encapsulation Mechanism)은 CRYSTALS-Kyber를 표준화한 암호 알고리즘으로, Module-LWE(Learning With Errors) 문제를 수학적 난제로 사용한다. ML-KEM은 대칭키 암호 통신에 사용하는 비밀 공유키 교환에 사용하며, 보안 강도에 따라 Table 1. 과 같은 키 크기를 갖는다.

Table 1. ML-KEM

	encapsulation key	decapsulation key	ciphertext	shared secret key
ML-KEM-512	800	1632	768	32
ML-KEM-768	1184	2400	1088	32
ML-KEM-1024	1568	3168	1568	32

2.1.2 ML-DSA

ML-DSA(Module Lattice-based Digital Signature Algorithm)는 CRYSTALS-Dilithium을 표준화한 암호 알고리즘으로, Module-LWE와 SelfTargetMSIS 문제를 수학적 난제로 사용한다. ML-DSA는 ML-KEM과 유사한 대수적 구조를 가진다[3]. ML-DSA는 부채널 공격에 내성을 갖도록 하기 위해 인스턴스 샘플링 시 Uniform Sampling만을 사용한다. ML-DSA는 보안 강도에 따라 Table 2.와 같은 키, 서명 크기를 갖는다.

Table 2. ML-DSA

	public key	private key	signature size
ML-DSA-44	2528	1312	2420
ML-DSA-65	4000	1952	3293
ML-DSA-87	4864	2592	4595

2.2 그리드 컴퓨팅

그리드 컴퓨팅은 공동 목표 달성을 위해 서로 다른 지리적 위치에 분산되어있는 컴퓨터 자원을 결합하는 컴퓨팅 인프라이다. 그리드 컴퓨팅을 통해 단일 컴퓨터로는 작업하기 어려운 대량 연산을 수행하거나 복잡한 문제를 해결할 수 있다. 현재 그리드 컴퓨팅 기술은 실시간 스트리밍 서비스 또는 비영리적 연구 프로젝트에 주로 활용되고 있다.

III. Post-Quantum Authentication and KEM Schemes in Grid Computing

1. 인증 및 키 교환 프로토콜에 대한 양자내성암호 적용

본 장에서는 그리드 컴퓨팅 환경에서의 사용자 인증 및 키 교환 프로토콜에 ML-DSA와 ML-KEM을 사용한다. 양자내성암호를 적용한 프로토콜을 통해 그리드 컴퓨팅에서 데이터 송수신 전에 신뢰할

수 있는 사용자인지 전자서명을 통해 검증하고, 암호키를 안전하게 교환하여 데이터 유출을 방지할 수 있다.

이 프로토콜에서 신뢰할 수 있는 서버는 Main Server, 그리드 컴퓨팅을 통해 컴퓨팅 자원을 받는 사용자는 User Node, 컴퓨팅 자원을 제공하는 사용자는 Supplier Node라고 한다.

1.1 사전 등록

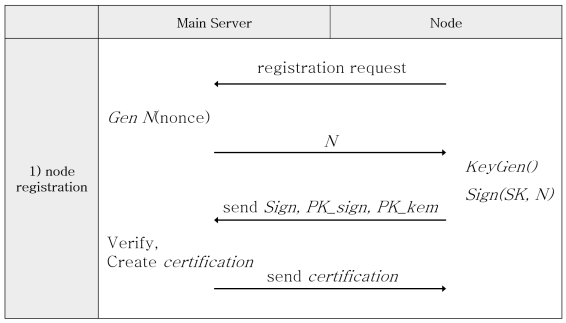

Fig. 2. node registration

그리드 컴퓨팅에 참여하는 사용자는 Fig. 2와 같이 신뢰할 수 있는 서버에 정보를 등록하고 인증을 통해 인증서를 발급받는다. 인증서는 해당 사용자가 서버의 인증을 받은 사용자임을 증명한다. 이후 서버는 사용자 간 P2P 통신 수립을 중개한다.

1.2. ML-DSA를 이용한 노드 인증

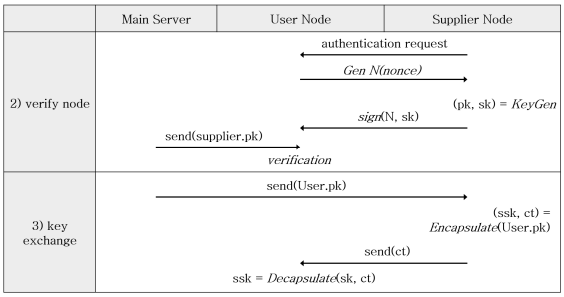

Fig. 3. authentication and key exchange Protocol

사용자의 자원 요청이 발생하면 서버의 중개를 통해 사용자 간 통신이 수립된다. 본격적인 그리드 컴퓨팅을 시작하기 전에 연결된 상대 노드를 신뢰할 수 있는지 확인한다. 이때 ML-DSA를 이용한 전자서명을 통해 노드 간 상호 인증이 이루어진다.

(1) 키 생성(Key Generation)

그리드 컴퓨팅에 참여하는 모든 사용자는 ML-DSA.KeyGen을 통해 공개키와 개인키 쌍을 생성하고 공개키를 서버에 등록한다.

(2) 인증 요청(Authentication Request)

사용자 인증을 위해 Fig. 3의 1)과 같이 피인증자(Supplier Node)가 인증자(User Node)에게 인증을 요청한다.

(3) Nonce 생성(Nonce Generation) 및 전달

인증 요청을 수신한 인증자는 Replay Attack 방지를 위해 무작위 Nonce를 생성해 전송한다.

(4) 서명 생성(Sign) 및 전달

피인증자는 ML-DSA.Sign 알고리즘에 개인 키와 수신한 Nonce를 입력하여 서명을 생성한다. 서명 후 인증자에게 서명을 전송한다.

(5) 서명 검증 (Verify)

서명을 수신한 인증자는 ML-DSA.Verify 알고리즘으로 서명을 검증한다. 공개키, Nonce 값, 그리고 서명을 대상으로 서명의 유효성을 확인한다.

1.3 ML-KEM 을 이용한 키 교환 및 데이터 암호화

1.2.에서 사용자 인증에 성공한 경우 대칭키 암호 통신을 위한 키를 교환한다. 인터넷 환경에서 안전한 키 교환을 위해 ML-KEM을 이용하여 키 교환 및 AES 암호화 프로토콜을 구현하였다.

(1) 키 생성 (Key Generation)

ML-KEM.KeyGen은 캡슐화 키(공개키)와 디캡슐화 키(개인키)를 생성한다. 캡슐화 키는 서버에 등록하여 키 교환 과정에 사용할 수 있도록 한다.

(2) 캡슐화 (Encapsulation)

키 교환을 위해서 Fig. 3의 2)와 같이 서버로부터 상대방의 캡슐화 키를 받은 다음, ML-KEM.Encaps 알고리즘에 의해 암호문과 비밀 공유키를 생성한다. 생성된 비밀 공유키는 본인이 소지하고, 암호문을 상대방에게 전송해 상대도 비밀 공유키를 획득할 수 있도록 한다.

(3) 디캡슐화 (Decapsulation)

암호문을 전달받은 당사자는 자신의 개인키를 이용해 이를 디캡슐화하여 비밀 공유키를 획득한다.

위 과정을 통해 두 통신 당사자 간 비밀 공유키가 분배되었으므로 사용자 간의 암호화 통신이 가능하다.

2. 성능 측정 및 결과

2.1 실험 환경

Table 3. experimental environment

OS	Windows, Linux
CPU	Intel(R) Core(TM) i7-1260P 2100Mhz
Memory Size	16GB

양자내성암호를 적용한 인증 및 키 교환 프로토콜의 성능 측정을 위해 Table 3과 같이 환경을 구성하였다. 구축한 실험 환경은 OS : Windows(User Node)/Linux(Supplier Node), CPU : Intel(R) Core(TM) i7-1260P 2100Mhz, Memory Size : 16GB이다. 위 환경에서 실험을 진행하며 연결 노드 수에 따른 사용자 인증 및 키 교환 과정의 소요 시간을 측정한다.

네트워크 환경의 차이로 인한 오차를 최소화하기 위해 하나의 기기에서 멀티스레딩을 통해 다수의 노드를 논리적으로 구성하고, 이들이 각각 인증 및 키 교환을 수행한다.

2.2 실험 시나리오

인증 및 키 교환 프로토콜의 성능 측정은 처음 사용자가 인증을 요청한 시점부터 인증 및 키 교환을 완료하고, 교환한 키(비밀 공유키)를 이용해 암호화된 데이터를 노드가 수신하여 복호화가 완료되는 데까지 걸리는 시간을 측정한다. 이때 연결되는 노드의 수를 1:1부터 시작해 1:5, 1:10, … 1:N과 같이 변화시키며 노드 수 증가에 따른 소요시간 변화를 측정한다.

소요시간 변화 측정을 통해 1:N으로 연결된 그리드 컴퓨팅 환경에서 기존 RSA, ECC를 대체한 양자내성암호 알고리즘이 적용된 인증 및 키 교환 프로토콜의 성능을 분석하고자 한다.

2.3 성능 측정 결과 분석

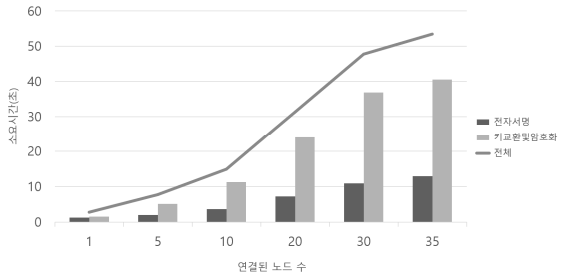

Fig. 4. Changes in time required based on the number of connected nodes

그리드 컴퓨팅 환경에서는 하나의 User Node(자원 요청자)에 다수의 Supplier Node(자원 제공자)가 연결되므로 Fig. 4는 Supplier Node 수의 증가에 따른 인증 및 키 교환 소요시간의 변화를 측정한 결과이다.

User Node에 연결된 Supplier Node가 1개인 경우 평균 2초 내외로 전자서명을 통한 인증 후 키 교환을 통한 암복호화가 완료되었으며, Supplier Node가 20개인 경우에는 평균 30초 이내, 35개인 경우에도 평균 1분 이내에 인증 및 키 교환이 이루어짐을 확인했다.

IV. Conclusions

본 논문에서는 그리드 컴퓨팅의 보안성을 강화하고 양자컴퓨터의 발전으로 인한 위협에 대응할 수 있도록 양자내성암호를 적용한 인증과 키 교환 프로토콜을 구현하고 성능을 측정하였다. 실험 결과 그리드 컴퓨팅 환경에서 인증과 키 교환은 최초 통신 수립 시 1회만 수행된다는 점을 고려하면 양자내성암호 적용에 따른 사용성 저하가 두드러지지 않음을 알 수 있었다.

따라서 본 연구를 통해 인증 및 키 교환 과정에 양자내성암호를 적용함으로써 그리드 컴퓨팅 시스템의 P2P 특성에서 기인하는 보안 문제를 해결하고, 기존에 주로 내부망이나 실시간 스트리밍 서비스에서 활용되던 그리드 컴퓨팅의 인터넷 환경으로의 확장 가능성을 제시한다. 향후 계획으로는 기존 공개키 알고리즘과의 성능 비교를 통한 프로토콜 최적화 방안에 관해 연구하는 것이 목표이다.

REFERENCES

[1] SeongWoo Lee, Tae-Shik Son, “Feasibility Study of Post Quantum Cryptography in TLS 1.3”, Journal of Digital Contents Society, 24(1), pp. 167-175, 2023.

[2] SunHong Hwang, “Discovery of Vulnerabilities in Live-Streaming service based on grid computing and research on countermeasures”, Graduate School Chonnam National University, Feb. 2022

[3] Sechang Jang, Minjong Lee, Hyoju Kang, & Jaecheol Ha, “A Study on Performance Improvement of Non-Profiling Based Power Analysis Attack against CRYSTALS-Dilithium”, Journal of the Korea Institute of Information Security & Cryptology, 33(1), pp. 33-43, Feb. 2023

[4] National Institute of Standards and Technology, “Module-Lattice-based Key-Encapsulation Mechanism Standard”, Federal Information Processing Standards Publication, August 24, 2023

[5] National Institute of Standards and Technology, “Module-Lattice-Based Digital Signature Standard”, Federal Information Processing Standards Publication, August 24, 2023